Fondamenti di Aritmetica - Compito del 26/06/2006

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Dimostrare che, per ogni $n \in \mathbb{Z}$, 16 divide $n^{12} - n^4$.
b) Calcolare l'ordine di 5 in $(\mathbb{Z}_{101})^*$.
c) Trovare a tale che $7|(5132a1135)_8$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 21x \equiv 42 \pmod{77} \\ 5x \equiv -1 \pmod{33} \\ 7x \equiv 19 \pmod{45} \end{cases}.$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ definita da $f(x) = 7x + 2$ la chiave per la codifica.
a) si verifichi che f è invertibile e si calcoli f^{-1};
b) si decodifichi la parola EGPYFEGP.

Esercizio 4. Siano P, $Q \in \mathbb{Q}[X]$ tali che $MCD(P, Q) \neq 1$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) P e Q non hanno radici in comune in $\mathbb{Q}$;
b) se P è irriducibile, allora $P|Q$;
c) P e Q hanno almeno una radice in comune in $\mathbb{Q}$;
d) se P e Q sono irriducibili, allora $P = Q$.

Esercizio 5. Si consideri l'anello $R = \mathbb{Z}_7[X]/(X^4 + 5X^2 - 1)$.
a) Se R è finito si dica quanti sono i suoi elementi. (motivare la risposta)
b) Fattorizzare X^4+5X^2-1 in $\mathbb{Z}_7[X]$. R è un campo ? (motivare la risposta)
c) Per ognuno dei seguenti elementi $Q \in R$ dire se è invertibile o un divisore di zero e trovare l'inverso o un elemento $S \in R - \{0\}$ tale che $QS = 0$ in R.
i) $Q = X^2 - 4$;
ii) $Q = X^2 + 4$;
iii) $Q = X^3 - 2X^2 - 2X + 4$.

Fondamenti di Aritmetica - Compito del 21/07/2006

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Per quali $a \in \mathbb{Z}$ l'equazione $21x + ay = 14$ ha soluzioni $x, y \in \mathbb{Z}$.
b) Calcolare il resto della divisione per 11 di $123456789^{987654321} - 123456789$.
c) Risolvere $5^x \equiv 4 \pmod{11}$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 15x \equiv 60 \pmod{35} \\ 5x \equiv -1 \pmod{21} \\ 4x \equiv -17 \pmod{99} \end{cases}.$$

Esercizio 3. Sia $(263, 17)$ la coppia (n, v) di un codice RSA.
a) Quale è l'esponente necessario per la decodifica ?
b) Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e si codifichi la parola VOTO con il codice dato.

Esercizio 4. Sia $P \in \mathbb{Z}_{11}[X]/(X^2 + 9X + 3)$ con $P \neq 0$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) se $P(-2) \neq 0$ allora P è invertibile;
b) se $P(-2) = 0$ allora P è un divisore di zero;
c) se P è invertibile allora $P(-2) \neq 0$ e $P(4) \neq 0$;
d) se P è un divisore di zero allora $P(4) = 0$.

Esercizio 5. Si consideri l'anello $R = \mathbb{Z}_7[X]/(X^4 - X^2 + 1)$.
a) R è un campo ? (Sugg. cercare fattorizzazioni con polinomi monici).
b) Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
i) $P = X^2 + 1$ è invertibile in R e $P^{-1} = X^2 - 2$;
ii) $P = X^2 + 1$ è invertibile in R e $P^{-1} = 2X^2 + 3$;
iii) $P = X^2 + 4$ è un divisore di zero in R e $P(X^2 + 2) = 0$.

Fondamenti di Aritmetica - Compito del 22/09/2006

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Trovare due distinte fattorizzazioni di $X^2 + 18$ in $\mathbb{Z}_{27}[X]$ come prodotto di polinomi lineari.
b) Dimostrare che per ogni $n \in \mathbb{Z}$ si ha che 9 divide $n^2(n^6 - 1)$.
c) Quale è il resto della divisione per 9 di $(53516023)_8$?

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 13x & \equiv & 19 & (\text{mod } 80) \\ 25x & \equiv & 10 & (\text{mod } 65) \\ 19x & \equiv & 5 & (\text{mod } 52) \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ definita da $f(x) = 5x + 11$ la chiave per la codifica.
a) Si verifichi che f è invertibile e si calcoli f^{-1};
b) si decodifichi la parola PLHXX.

Esercizio 4. Sia $P = X^2 - X + 1 \in \mathbb{Z}_7[X]$ e sia $Q \in \mathbb{Z}_7[X]$ tale che $MCD(P, Q) \neq 1$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) Q divide P;
b) se Q è irriducibile allora deg $Q = 1$;
c) $Q(3) = 0$ o $Q(5) = 0$;
d) $Q(3) = 0$ e $Q(5) = 0$.

Esercizio 5. Si consideri l'anello $R = \mathbb{Z}_{11}[X]/(X^3 + 3X^2 - 2X - 6)$.
a) Se R è finito si dica, motivando la risposta, quanti sono i suoi elementi.
b) Si dica, motivando la risposta, se R è un campo.
c) Per ognuno dei seguenti elementi $Q \in R$ dire se è invertibile o un divisore di zero e trovare l'inverso o un elemento $S \in R - \{0\}$ tale che $QS = 0$ in R.
i) $Q = X^2 - 2$;
ii) $Q = X^2 + 2$;
iii) $Q = X^2 + 5X + 6$.